

TEACH AGENTS WHEN NOT TO ACT

Practicing Agentic DevOps

Intent defines the outcome.
Policy defines the authority.
Humans own the exceptions.

Kamesh Sampath

Lead Developer Advocate | Snowflake



Kamesh Sampath

Lead Developer Advocate



```
# The Core Profile: Infrastructure as a Person
innovator:
  identity: "Veteran Tech Innovator"
  experience: "years ≥ 20 in the trenches"
  specs:
    - Author
    - Developer Advocate
    - Core Infrastructure Architect
    - linkedin.com/in/kameshsampath

# Runtime Parameters
mission:
  target: "Empower developers to build the impossible"
  strategy: "Demystify complex data & cloud ecosystems"
```



Safe Harbor and Disclaimers

Other than statements of historical fact, all statements contained in these materials and any accompanying oral commentary (collectively, the “Materials”) are forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended, including statements regarding (i) Snowflake’s business strategy, plans, opportunities, or priorities; (ii) Snowflake’s new or enhanced products, services, and technology offerings, including those that are under development or not generally available; (iii) market size and growth, trends, and competitive considerations; (iv) Snowflake’s vision, strategy, and expected benefits relating to artificial intelligence (“AI”), Snowpark, Snowflake Marketplace, the AI Data Cloud, and AI Data Clouds for specific industries or product categories, including the expected benefits and network effects of the AI Data Cloud; and (v) the integration, interoperability, and availability of Snowflake’s products, services, or technology offerings with or on third-party platforms or products, including public cloud platforms. These forward-looking statements are subject to a number of known and unknown risks, uncertainties, and assumptions, including those described under the heading “Risk Factors” and elsewhere in the Annual Reports on Form 10-K and the Quarterly Reports on Form 10-Q that Snowflake files with the Securities and Exchange Commission from time to time. In light of these risks, uncertainties, and assumptions, the future events and trends discussed in the Materials may not occur, and actual results could differ materially and adversely from those expressed or implied in the forward-looking statements. As a result, you should not rely on any forwarding-looking statements as predictions of future events. Forward-looking statements speak only as of the date the statements are first made and are based on information available to Snowflake at the time those statements are made and/or management's good faith belief as of that time. Except as required by law, we undertake no obligation, and do not intend, to update the forward-looking statements in these Materials.

Any future product or roadmap information (collectively, the “Roadmap”) is intended to outline general product direction. The Roadmap is not a commitment, promise, or legal obligation for Snowflake to deliver any future products, features, or functionality; and is not intended to be, and shall not be deemed to be, incorporated into any contract. The actual timing of any product, feature, or functionality that is ultimately made available may be different from what is presented in the Roadmap. The Roadmap information should not be used when making a purchasing decision. In case of conflict between the information contained in the Materials and official Snowflake documentation, official Snowflake documentation should take precedence over these Materials. Further, note that Snowflake has made no determination as to whether separate fees will be charged for any future products, features, and/or functionality which may ultimately be made available. Snowflake may, in its own discretion, choose to charge separate fees for the delivery of any future products, features, and/or functionality which are ultimately made available.

The Materials may contain information provided by third-parties. Snowflake has not independently verified this information, and usage of this information does not mean or imply that Snowflake has adopted this information as its own or independently verified its accuracy.

REV 12.16.25



The Bot Did What I Asked

I had not told it what it was allowed to do.

02:00

PRODUCTION INCIDENT

A BUILDER'S STORY

"Find bugs and fix them."

- 01 Bot identifies a concurrency issue.
- 02 Its proposed fix removes a lock.
- 03 The change reaches production.

An outcome is not an authorization boundary.



Separate Intent From Authority

Turn 'find bugs and fix them' into an explicit contract.

01

WHAT SHOULD BE TRUE?

Intent

Find defects. Preserve behavior.
Produce evidence and a proposed change.

02

WHAT MAY CHANGE?

Policy

Define allowed files, fix ceilings, and actions that must stop.

03

WHO DECIDES?

Human review

Assess uncertainty. Approve a specific next step, not unlimited access.

A useful refusal explains the risk and the next decision.



Low Risk Is A Conjunction

Conservative means all three conditions must hold.

LOW severity

AND

LOW complexity

AND

HIGH confidence

All three match

Prepare a fix PR/MR.

Keep merge approval separate.

Any condition fails

Label needs-review.

Explain the evidence and uncertainty.

Model confidence is an assessment, not a calibrated probability.



CI Carries The Action Boundary

Use the runner for execution, not as a blanket grant of authority.

01

IDENTITY

Authenticate

OIDC: short-lived identity, no stored secrets.

02

TWO CLIS

Execute

snow for commands. cortex for agent tasks.

03

DELIVERY

Review

Tests, PR/MR approval, then deployment.

Secretless Snowflake authentication does not mean unrestricted execution.



Agentic DevOps Reaches Database State

The same operating model applied to database state.

01

DEFINE

Desired object state

02

PLAN

CREATE / ALTER / DROP

03

REVIEW

Revision and target

04

DEPLOY

Authorized changes

Proposed CI gate: stop on a destructive change.

The scope expands. Intent, policy, and human review still apply.



Keep The Boundary Across Platforms

Same routing idea. Different repository and review mechanics.

GITHUB ACTIONS

Issue to pull request

`/coco fix`

Developer requests a fix.
Review the resulting PR.

Snowflake CLI Action: GA

GITLAB CI

Issue to merge request

`@coco-agent fix`

Duo triggers the agent.
Review the resulting MR.

Snowflake CLI component: Public Preview

Approve a fix proposal without granting automatic merge or deploy.



Watch The Agent Stop

Scaffold. Scan. Score. Propose. Escalate.

Live-demo runbook

- 1. Scaffold an isolated sandbox.
- 2. Show the conservative policy.
- 3. Push low-risk and risky defects.
- 4. Inspect auto-fix vs needs-review.
- 5. Authorize one scoped next step.

DCM checkpoint: review a DROP; withhold deployment.

Policy ceiling

conservative

Complexity

low

Severity

low

Confidence

high

 POLICY DECISION

auto-fix

Low severity, low complexity, and high confidence meet the conservative ceiling.
Propose a fix PR/MR; do not merge or deploy.

Interactive illustration only. No agent, repository, or database operations are executed.



The Goal Is Bounded Action

Not a CI bot that always acts.

01

Intent defines the outcome.

State what should be true.

02

Policy defines the authority.

Constrain what can change.

03

Humans own the exceptions.

Review uncertainty before escalation.

Teach agents to explain why they proceeded - or stopped.



CoCo Brings Data Context To Code

Not another coding agent.

01

CONTEXT

Understand

Link code intent to Snowflake objects.

02

CAPABILITY

Build

Read, edit, and run development tools.

03

EVIDENCE

Verify

Run checks within granted access.

Context helps the agent decide. Permissions bound its reach. Your data stays in your account.



An Agent Can Change Repository State

The moment it acts, instructions become part of delivery design.

01

INTENT

Teach the workflow

Project conventions live in the repo.

02

ACTION

Connect the tools

Scan, edit, and open PRs or MRs.

03

BOUNDARY

Constrain the authority

Scope credentials. Require review.

Instructions guide behavior. Enforced controls restrict authority.



Start With One Bounded Workflow

Demo recording, docs, and templates

01 Watch the full demo
[youtu.be](#)

03 CoCo CLI security
[docs.snowflake.com](#)

05 Snowflake Actions
[github.com](#)

07 GitHub agent template
[github.com](#)

09 GitLab CI/CD component
[gitlab.com](#)

11 Plan and deploy DCM
[docs.snowflake.com](#)

02 CoCo overview
[docs.snowflake.com](#)

04 Snowflake CLI CI/CD
[docs.snowflake.com](#)

06 DevOps CoCo Agents
[github.com](#)

08 GitLab agent template
[gitlab.com](#)

10 DCM Projects
[docs.snowflake.com](#)

